A Report
to the
Montana
Legislature

Information Systems Audit

Improving Controls Over Security of Laptop Data

Department of Justice
Department of Labor and Industry
Department of Public Health and Human Services
Department of Revenue

January 2012

Legislative Audit
Division

11DP-12

Information Systems Audits

Information Systems (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. We conducted this IS audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objectives.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting, education, computer science, mathematics, political science, and public administration.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

Audit Staff

Deon Olson
Kent Rice
Nathan Tobin

Reports can be found in electronic format at:
http://leg.mt.gov/audit

LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Deborah F. Butler, Legal Counsel

Deputy Legislative Auditors
Cindy Jorgenson
Angie Grove

January 2012

The Legislative Audit Committee
of the Montana State Legislature:

We conducted an Information Systems audit of laptop data security at Departments of Justice, Labor and Industry, Public Health and Human Services, and Revenue. The overall purpose was to verify if existing controls ensure adequate security of sensitive data on laptops.

Overall, we identified laptops throughout all four agencies that are vulnerable to potential security breaches. We issued recommendations for agencies to improve security controls, including periodic monitoring of laptop security settings, improving user awareness of security policies and procedures, ensuring encryption of sensitive laptop data, and limiting the use of laptops.

We wish to express our appreciation to personnel within all four departments for their cooperation and assistance.

Respectfully submitted,

/s/ Tori Hunthausen

Tori Hunthausen, CPA
Legislative Auditor

Room 160 • State Capitol Building • PO Box 201705 • Helena, MT • 59620-1705
Phone (406) 444-3122 • FAX (406) 444-9784 • E-Mail lad@mt.gov

Table of Contents

Figures and Tables

Figures

Tables

Appointed and Administrative Officials

Department of Justice	Steve Bullock, Attorney General
	Tim Burton, Chief of Staff
	Joe Chapman, Chief Information Officer
Department of Labor and Industry	Keith Kelly, Commissioner
	George Parisot, Chief Information Officer
	Judy Kelly, OIT Bureau Chief
Department of Public Health and Human Services	Anna Whiting Sorrell, Director
	Laurie Lamson, Operations Services Branch Manager
	Ron Baldwin, Chief Information Officer
	Teri Lundberg, Networks and Communications Bureau Chief
Department of Revenue	Dan Bucks, Director
	Alan Peura, Deputy Director
	Margaret Kauska, IT/Processing Administrator

MONTANA LEGISLATIVE AUDIT DIVISION

INFORMATION SYSTEMS AUDIT
Improving Controls Over Security of Laptop Data
Department of Justice, Department of Labor and Industry, Department of Public Health and Human Services, Department of Revenue

JANUARY 2012 11DP-12 REPORT SUMMARY

Laptops comprise almost 25 percent of all computers used in Montana state government. Laptops provide for added mobility, but they also present an increased risk to data security. Current controls do not ensure an adequate level of security for all data within the departments reviewed.

Context

During recent years, use of laptop computers within state government has steadily increased. The 2011 Biennial IT Report states laptops make up 23 percent of all computers compared with 14.6 percent for the previous biennium. Overall, the State Information Technology Services Division reports 3,431 laptops in service throughout state government, excluding the university system. Reasons for the rise in laptop use are their portability and ability to connect remotely to the state network. This provides laptop users the flexibility to travel for work and maintain communication with their offices.

While laptops allow for added mobility and flexibility, they also present added data security risks. Because they are portable, laptop computers are often outside the physical security of state offices and at risk of loss or theft. This becomes critical when laptops are used to service and store confidential data, increasing the need for added physical and data security. Because of the heightened security risk, we conducted an audit to identify and test laptop security controls to verify security of sensitive data. To achieve our objective, we developed testing protocol based on statute, best practices, and state policy and tested a sample of 100 laptops at four different agencies.

Results

Overall, we identified laptops throughout all four agencies that are vulnerable to potential security breaches. We issued recommendations for agencies to improve security controls, including periodic monitoring of laptop security settings, improving user awareness of security policies and procedures, ensuring encryption of sensitive laptop data, and limiting the use of laptops.

(continued on back)

Recommendation Concurrence	
Concur	3
Partially Concur	0
Do Not Concur	0

Source: Agency audit response included in final report.

For a complete copy of the report (11DP-12) or for further information, contact the Legislative Audit Division at 406-444-3122; e-mail to **lad@mt.gov**; or check the web site at **http://leg.mt.gov/audit**
Report Fraud, Waste, and Abuse to the Legislative Auditor's FRAUD HOTLINE
Call toll-free 1-800-222-4446, or e-mail **lad@mt.gov**.

Chapter I – Introduction

Introduction

During recent years, use of laptop computers within state government has steadily increased. The 2011 Biennial IT Report states laptops make up 23 percent of all computers compared with 14.6 percent for the previous biennium. Overall, the State Information Technology Services Division reports 3,431 laptops in service throughout state government, excluding the university system. Reasons for the rise in laptop use are their portability and ability to connect remotely to the state network. This provides laptop users the flexibility to travel for work and maintain communication with their offices.

While laptops allow for added mobility and flexibility, they also present added data security risks. Because they are portable, laptop computers are often outside the physical security of state offices and at risk of loss or theft. This becomes critical when laptops are used to service and store confidential data. All computers require some level of security, but because laptops are portable and can contain sensitive data, the need for added physical and data security is heightened. Because of the heightened security risk, we conducted an audit over laptop data security.

Audit Objective and Methodologies

Agencies should implement data security controls that meet minimum requirements and guidelines established in statute, policy, and best practices. For this audit, our objective was to determine if controls are in place to adequately secure sensitive data on laptops.

To conclude on our objective, we developed and performed testing on laptop computers at four agencies within state government. To achieve this, we selected a sample of laptops for testing, and developed testing protocol based on best practices and state policy. Audit work was conducted in accordance with Government Auditing Standards published by the United States Government Accountability Office.

Agencies Selected

We obtained a statewide inventory of laptops from the Department of Administration to determine the number of laptops at the various agencies. The inventory showed over 3,400 laptops in use at 34 entities, excluding the university system. Due to the overall number of laptops and state agencies, we determined it was not feasible to review controls for every laptop. For this reason, we decided to select a sample for review. We chose four agencies from the top ten in laptop use for the state that also

work with confidential and sensitive information, including public health, tax-related, criminal justice, and employment records.

Our sample of agencies included the Department of Revenue (DOR), Department of Public Health and Human Services (DPHHS), Department of Labor and Industry (DLI), and Department of Justice (DOJ). However, the laptop data security controls addressed in this audit are applicable to all agencies with laptops.

Laptop Sample

Once we identified the sample agencies, we obtained an inventory of laptops from each individual agency to obtain a more current and accurate depiction of the number of laptops in use and where they are located. Table 1 shows the number of laptops at each agency.

Table 1
Laptops per Agency

Agency	Number of Laptops
DOJ	341
DLI	515
DOR	388
DPHHS	648
Total	**1892**

Source: Compiled by the Legislative Audit Division based on agency data.

We selected a judgmental sample of 100 laptops for testing. Considering the mobility of laptops, our sample included laptops in cities throughout Montana, including Billings, Boulder, Helena, Butte, Bozeman, and Missoula. We also chose laptops from different programs and divisions within each agency to sample a broader spectrum of use.

Testing Protocol

Once we selected our sample, we established a protocol to verify data security implemented at each agency. We began by identifying controls related to securing laptop data in available statute, policies, and best practices. Our review included statewide IT policies that address mobile computing and working with sensitive data and guidelines put forth by the National Institute of Standards and Technology and Control Objectives for Information and related Technology.

We identified key controls that should be in place to ensure an adequate level of security. We then developed a methodology to verify those controls were present on each laptop. Table 2 provides a list and description of each control area tested. Additional information on these controls can be found in Appendix A. Each of the items identified in the following table are important security controls and we expected compliance in each control area. A laptop with a single control missing is vulnerable to data loss or damage.

Table 2
Testing Control Areas

Test	Explanation
BIOS Settings	Require a password protecting the BIOS (basic input/ output system).
Generic/Administrative Authentication	Assign unique usernames and passwords for access to computers and the state network.
Patching	Ensure current critical security patches are applied.
User Account Setup	Assign a user account unique to a single user. Deactivate generic, disable guest accounts and rename administrative accounts.
Auto Locking	Require computers to have a screen saver with password protection enabled.
Account Password Settings	Require passwords to be at least 6 – 8 characters in length, changed every 60 days, and consist of different character types.
Account Lockout Thresholds	Require the account lockout threshold be enabled on user accounts.
Access Audit Policies	Log both successful and unsuccessful access attempts.
File System Structure	Ensure all hard drives are formatted NTFS (New Technology File System) for Windows based machines.
Simple File Sharing	Disable this function.
Microsoft Office	Security settings be set to not trust Macros, Add-ins and Templates, or Visual Basic (VB) Project.
Windows Messenger	Disable this service.
Internet Connection Sharing	Disable this service.
Firewall	Enabled firewalls on all laptops.
Anti-virus	Install active and current anti-virus definitions.

Source: Compiled by the Legislative Audit Division.

User Interviews

The final element of our audit testing involved meeting with the users assigned the laptops in our sample. As part of our methodology, we created a standard list of questions to ask if users:

- Are aware of existing policies and procedures related to laptop security?
- Work with sensitive or confidential information?
- Save sensitive or confidential information to the hard drive of their laptop?
- Connect to networks outside the state network?
- Secure their laptop when left unattended?
- Frequently use laptops outside their office?

We interviewed 84 users throughout the agencies. The difference between the number of laptops tested and number of users interviewed was due to laptop use. Some of the laptops in our sample are part of a pool of laptops which can be checked out by staff, but are not assigned to a unique user. Some laptops are assigned specifically to a room rather than a user.

Area for Further Study

During the course of the audit, we identified an area we believe warrants consideration for future Information Systems audit work.

Laptop Data Security within the Montana University System (MUS)

At the beginning of this audit, we assessed the use of laptop computers within state government. During our assessment, we contacted the two main university campuses (MSU-Bozeman and UM-Missoula) to obtain information regarding the use of laptops on their respective campuses. We identified weaknesses with inventory control at both institutions, and were unable to obtain the actual number of laptops in use within the MUS. As a result, we excluded the MUS from this audit. A future Information Systems audit could evaluate laptop data security controls within the MUS similar to the work conducted during this audit.

Chapter II – Findings and Recommendations

Introduction

Overall, we identified laptops throughout all four agencies that are vulnerable to potential security breaches. Application of controls is inconsistent within each agency and compliance with state policy and best practices could be strengthened. Vulnerable laptops included those which have the potential to be used to modify and store sensitive data such as:

- Employee Social Security Numbers
- Criminal Investigation Documentation
- Individual Tax Records
- HIPAA Protected Healthcare Records

Because of the lack of controls and resulting risk to data, not only is laptop data vulnerable but agencies could strengthen compliance with state security policy and state statute. The remainder of this report discusses our findings and includes recommendations to improve laptop security, including monitoring of laptops to ensure consistent implementation of security controls, improving user awareness, implementation of data encryption, and limiting laptop use.

Evaluation of Laptop Data Security

To evaluate laptop data security at the agencies, we obtained the location of all laptops identified in our sample and the names of the users assigned those laptops. We met with each user to test the laptop and conduct an interview. Our laptop tests followed the testing methodology described in the first chapter and consisted of automated security scans in conjunction with manually verifying security configurations.

Overall, our audit results identified noncompliance at each agency; however, the control areas and number of exceptions varied. Table 3 shows areas of noncompliance identified at each agency. If we identified any laptop with a security control weakness, the agency was not providing an adequate level of data security and receives an "X" in the following table indicating noncompliance with state policies and/or best practices. Of the fifteen control areas tested, only four had comprehensive security controls in place, while nine control areas were missing at a majority of the agencies.

Table 3
Areas of Noncompliance per Agency

Test	DLI	DOJ	DOR	DPHHS
BIOS Settings	X	X	X	
User Authentication				
Patching	X	X	X	
Generic/Admin Accounts	X	X	X	X
Auto Locking	X	X	X	X
Account Password Settings	X	X	X	
Account Lockout Thresholds	X	X	X	
Access Audit Policies	X	X	X	
File System Structure				
Simple File Sharing	X	X	X	X
Microsoft Office	X	X		
Windows Messenger				
Internet Connection Sharing				
Firewall	X		X	
Anti-Virus	X	X		X

Source: Compiled by the Legislative Audit Division based on testing of agency laptops.

DPHHS has made the most progress toward securing data on laptops, implementing a security software suite that allows for full encryption over all its laptops, as well as an interface to centrally manage security settings. As a result, our testing at DPHHS identified the least amount of noncompliance among the agencies. It is important to note that while DPHHS has made progress, each agency has different organizational structures and resources, so one agency's environment may not work for the others.

Summary

Each of the control weaknesses we identified could potentially be used to compromise sensitive data. The risk increases when considering the staff at all four agencies save sensitive or confidential data to their laptops. In fact, roughly 40 percent of the users we interviewed save what they considered sensitive data to their laptops. Although each agency is aware of security controls, they could improve consistent application among all laptops.

Agencies Should Monitor Laptop Security Settings

State statute (§2-15-114, MCA) places the responsibility for an adequate level of security for all agency data with the department head. At each agency, laptop security has been tasked to IT staff, who establish laptop security configurations. While laptops may initially be secure, over time settings can be altered or become outdated. In order for agencies to comply with statute, they need to ensure laptops remain secure once assigned to users. However, the ongoing management of laptops is often the responsibility of the assigned user or IT staff within a particular division. Once management of laptops is assigned to a user, it becomes difficult to determine if security controls are not working or have been modified.

Currently, agencies could improve proactive monitoring of laptops to identify where security controls are outdated or have been altered. All of the agencies sampled have or are taking steps to centralize agency IT management, limit administrative access, and develop consistent settings for each laptop. However, based on our testing results, these actions have not assured secure laptop controls.

Laptops lacking security controls remain at risk and there is the potential that various security vulnerabilities result in loss of sensitive data. A number of the users we spoke with work from home or remotely for periods of time. Without current or accurate security settings, and outside the protection of the state network, these laptops are vulnerable to threat or breach of data. Proactive and routine monitoring would allow agencies to identify when security settings are not functioning as expected and address vulnerabilities.

Laptop Users Not Aware of Security Policies

For agencies to provide an adequate level of security, state statute requires agencies to develop internal policies and procedures to ensure data security. Another critical element of laptop data security is the responsibility of users to follow those policies and procedures. Of the 84 laptop users interviewed during this audit, 50 percent were not aware of related policy or procedure, even though the agencies have policies relating to computer use and managing sensitive data. Although most users are typically aware of general elements of laptop security, such as physically securing laptops when out of the office, they are not aware of other key existing policies, procedures, and best practices.

Most users recall receiving some policy documents when they first started work or when they received their laptop. However, users could not recall receiving training over policy details and policy information is often not reinforced. If a user is not aware of security policies and procedures, their actions could potentially lead to security vulnerabilities. For example, 12 users we interviewed indicated they have accessed an

unsecure network and that they store sensitive data on the hard drive of their laptop where other users could use the shared network to access the laptop hard drive. In addition, all agencies have reported at least one lost or stolen laptop within the past three years.

Without knowledge of data security procedures, users may be unaware of or remove applied security settings, leaving the contents of the laptop open to unauthorized users. Security policies and procedures should be continually reinforced to increase user awareness to help minimize security vulnerabilities and ensure compliance with statute and policies regarding laptop security.

RECOMMENDATION #1

We recommend the agencies:

A. *Routinely monitor laptop security settings to ensure application of security controls.*

B. *Improve and maintain user awareness of laptop security policies and procedures.*

Agencies Need to Improve Encryption Procedures

One measure agencies can take to mitigate the risk of inadequate security controls is to encrypt sensitive data. Even if a laptop is lost or stolen, encrypting data makes it unreadable, preventing access from unauthorized sources. State policy requires encryption of any sensitive data that leaves state property (is taken off the state network). There are several different means of data encryption, including:

- Hard Drive Encryption – Encrypts all files saved to a computer hard drive. Encryption is unlocked when an authorized user logs onto the device.
- Folder Encryption – Encrypts all files saved to a designated folder. Login credentials are required to open an encrypted folder.
- File Encryption – Individual files are encrypted. Login credentials are required to open an encrypted file.
- Application Encryption – A computer application automatically encrypts any files or data created using the application. Encryption is unlocked when an authorized user logs into the application.

Complete hard drive encryption guarantees data is encrypted regardless of user actions. Both folder and file encryption require user participation by saving to the correct folder or manually encrypting files. Folder encryption can be customized

to require users to save to encrypted folders by default, which helps minimize user interactions. Application encryption is automatic, but only affects files created through the application and does not apply to other files and data on a laptop.

All sampled agencies are implementing some level of encryption, but the effectiveness varies. DPHHS has installed full hard drive encryption on every laptop. DOR has installed an encrypted folder on each machine. However, 6 of 12 users we interviewed were unaware it was available. DLI indicates they have full hard drive encryption available in specific divisions, but our testing did not identify any laptops with encryption. DOJ encrypts all data created through the Criminal Justice Information Network application, but does not account for other files saved to laptops.

It should be noted that because DPHHS is encrypting all data through full hard drive encryption, several of the security control tests we completed were mitigated. In addition, DPHHS recently lost a laptop with sensitive data, but because they implemented encryption of all files, the security of data should have been maintained. This level of encryption costs about $120 for each machine, plus a $25 yearly fee. However, there are currently other less expensive options for agencies to employ. For example, DLI provides select staff with use of a free file encryption software. In addition, the cost associated with laptop encryption is minimal compared with the potential cost associated with a data breach, which has been estimated to cost over $20,000 for a single lost laptop.

By improving existing practices to ensure encryption of sensitive data on laptops, agencies will strengthen data security and limit the risk that agency data will be unprotected if the laptop is compromised.

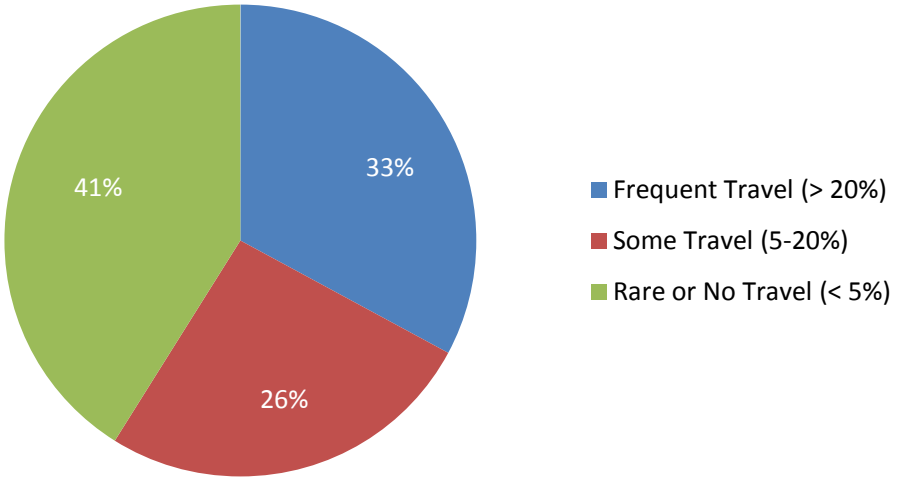
RECOMMENDATION #2

We recommend the Department of Labor and Industry, Department of Justice, and Department of Revenue take steps to ensure compliance with state policy by implementing or improving procedures to ensure sensitive data on laptops is encrypted.

Agencies Could Further Analyze Need for Laptops

One of the more effective ways to limit the risks associated with laptop computers is to limit their use. Of the 84 users interviewed for this audit, 41 percent rarely used their laptops outside of the office, only traveling a couple of days a year at most. Figure 1 shows the frequency laptops are used outside the offices for those interviewed.

Figure 1
Laptops Usage Outside of State Offices



Source: Compiled by the Legislative Audit Division based on interviews with agency laptop users.

If mobility is not required, a desktop computer provides a more secure option. In addition, statute (§2-17-505, MCA) states it is the policy of the state that the development of information technology resources in the state must be conducted in an organized, deliberative, and cost-effective manner. Not only do laptops present added risk, they are also typically more expensive than their desktop counterparts. Based on agency information, laptops cost an average of $550 more than a comparable desktop. Based on those users that rarely travel, we identified $18,700 in potential savings if desktops were used instead. Further research noted laptops tend to experience higher maintenance costs and tend to have a shorter life cycle, both of which increase cost. However, evaluating the need for a laptop goes beyond cost-effectiveness.

Most of the users we interviewed were given laptops because supervisors believed staff need to travel. However, some users indicated they rarely work out of the office, or when they do, they do not require a computer. Even in instances where a laptop may be required, each agency has a pool of laptops that can be checked out for temporary use. While there is a process at each agency to request a laptop, we did not identify any analysis to verify need, security, or cost-effectiveness of the laptop. To limit security risk and decrease costs, agencies should analyze business need, security risk, and cost-effectiveness for laptop assignment.

RECOMMENDATION #3

We recommend the agencies analyze business need, security risk, and cost-effectiveness prior to assignment of laptops.

Appendix A

Laptop Control Areas

This section provides additional information about the control areas tested during this audit, including an explanation of how they should be configured based on policies and best practices.

BIOS Settings – The BIOS (basic input/output system) is the computer program responsible for the initial boot-up process when a computer is first turned on. Access to the BIOS would allow an intruder to bypass login requirements and have direct access to laptop content. Best practices suggest requiring a password to access the BIOS settings.

User Authentication – One critical security control requires a unique user name and password to access content on a laptop. Without this control, an unapproved individual would have direct access to content on a lost or stolen laptop. Limiting access to a computer by requiring users to login with a unique username and password is the primary method for controlling who can access the contents of a computer. State policy mandates all state laptops to require a username and password.

Patching – Microsoft periodically releases critical or important security patches designed to fix vulnerabilities in the Windows operating system or Microsoft Office. State policy requires critical security patches to be current. SITSD approves patches that are distributed by agencies.

Generic/Administrative Account Setup - One important aspect of assigning a user account is accountability, so user accounts should be unique to a single user. Generic accounts in use by multiple users limit the ability to identify who has accessed a laptop. In addition, it is also difficult to manage who has access through the generic account. Even more critical is the use of default guest and administrator accounts that are default to Windows operating systems. These are well-known accounts that allow access to modify or remove security settings. Best practices recommend disabling generic and administrative accounts.

Auto Locking - State policy requires computers to have a screen saver with password protection enabled on them. Best practices and state policy recommends the screen saver wait period be set to no more than 15 minutes.

Account Password Settings – State policy requires passwords to be at least 6 – 8 characters in length and to be changed every 60 days. In addition, passwords with

different character types limit the likelihood it can be guessed or identified through use of password identification software.

Account Lockout Thresholds and Access Audit Policies – Best practices suggest locking a computer after a number of failed attempts. This prevents unauthorized access. Otherwise the user can use password identification software to crack the password. Best practices also suggest additional security including logging access attempts so IT staff can identify when unauthorized access attempts have taken place, as well as assisting in identifying possible successful logins by unauthorized users.

File System Structure – For newer Microsoft Windows operating systems, there are two possible methods for creating a file structure: NTFS and FAT32. FAT32 is an older file structure and presents security vulnerabilities. NTFS is a new file structure and has been configured to provide better security controls. Best practices recommend using NTFS.

Simple File Sharing – Simple File Sharing is a feature provided by Microsoft allowing access to files and folders to other computers within your network. The risk increases when users are out of the state network and using an unsecured wireless network, such as at a hotel or coffee shop. Unauthorized users can easily access these unsecured networks and use the Simple File Sharing feature to access files on a state laptop. Best practices recommend this feature should be disabled.

Microsoft Office – Laptops with low security settings in Microsoft Office are vulnerable to a variety of external attacks. Certain tools and scripts such as Macros, add-ins, and Visual Basic projects can be exploited by viruses, trojans, and worms. Best practices recommend security settings be set to not trust Macros, Add-ins and Templates, or Visual Basic projects.

Windows Messenger and Internet Connection Sharing – Windows Messenger and Internet Connection Sharing are services that are included in Windows operating systems. When enabled, they allow remote communication with other computers, which could allow a remote party to access files on a laptop, as well as access the network the laptop is connected to. Best practices recommend disabling these services.

Firewall - Windows firewall is software that monitors and limits incoming and outgoing information to and from a computer. A firewall acts as a protective sweater, insulating computers from the outside and preventing hackers or malicious software from gaining access to your computer through a network or the Internet. If a laptop becomes infected, a firewall can prevent it from sending malicious software to other computers. State policy requires firewalls to be enabled on all computers.

Anti-virus – Anti-virus is software used to prevent, detect, and remove malicious software such as viruses and malware. As new viruses are detected, anti-virus definitions should be updated to address the threat. State policy requires all state computers to be installed with active and current anti-virus protection.

Departments' Responses

Department of Justice

Department of Labor and Industry

Department of Public Health and Human Services

Department of Revenue

ATTORNEY GENERAL
STATE OF MONTANA

Steve Bullock
Attorney General

Department of Justice
215 North Sanders
PO Box 201401
Helena, MT 59620-1401

January 25, 2012

Ms. Tori Hunthausen
Legislative Audit Division
PO Box 201705
Helena, MT 59620-1705

RE: Laptop audit response

Dear Ms. Hunthausen:

Enclosed please find the responses to the recommendations from the recent information technology audit conducted by your office for the Montana Department of Justice.

I want to personally thank you and your staff for undertaking this project. The review has been a positive experience and will ensure the continued protection of critical information. Feel free to contact me if you have any other questions or concerns. Thank you.

Sincerely,

STEVE BULLOCK
Attorney General

SB:sj

Recommendation #1:

We recommend the agencies:

A: Routinely monitor laptop security settings to ensure application of security controls.

We concur. The Montana Department of Justice (DOJ) is in the process of implementing a capability that will allow remote laptop monitoring from a central location which will be complete by December 2012. This central remote management will allow logging, application & operating system security controls, and timely critical system and antivirus updates in a timely manner. Until this capability is fully deployed, DOJ has implemented a routine manual review of laptops that are not centrally managed. Timeline: February 2012 - November 2012.

B: Improve and maintain user awareness of laptop security policies and procedures.

We concur. DOJ was already in the process of re-designing the security awareness training program for the department. The new training curriculum will include topics for mobile device security, such as: physical protection, software/system security settings, traveling with a device, saving folders and files, passwords and advanced authentication, public connection safety (WIFI) and encryption. In addition, DOJ will create a laptop user email group to continuously remind laptops users of correct policies and procedures. Timeline: February 2012 – May 2012

Recommendation #2:

We recommend the ... Department of Justice ... take steps to ensure compliance with state policy by implementing or improving procedures to ensure sensitive data on laptops is encrypted.

We concur. DOJ will, as part of the steps outlined above, include training and communication to users so that they will use centralized network file storage whenever possible. Our goal is to create a secure environment that users can store their sensitive files, so that they can access those files from any device without storing them on a laptop. DOJ will also include training and solutions to assist users with encrypting sensitive files that must reside on laptops due to business requirements. Timeline: February 2012 – May 2012

Recommendation #3:

We recommend the agencies analyze business need, security risk, and cost-effectiveness prior to assignment of laptops.

We concur. DOJ currently requires that supervisors approve laptops for employees. DOJ will require supervisors to also consider security when making this decision. Timeline: February 2012

Montana
Department of Labor and Industry
Commissioner's Office

BRIAN SCHWEITZER, GOVERNOR
KEITH KELLY, COMMISSIONER

January 26, 2012

RECEIVED
JAN 26 2012
LEGISLATIVE AUDIT DIV.

Tori Hunthausen, CPA
Legislative Auditor
State Capitol Building
PO Box 201705
Helena MT 5960-1705

Subject: Information Systems Audit #11DP-12: Improving Controls over Security of Laptop Data

Dear Ms. Hunthausen:

The Department of Labor and Industry has reviewed the January 2012 Information Systems Audit which focused on the security of laptop data in the Department and other state agencies. The Department would like to thank audit staff for their review. As a Department we are always looking for ways to improve and appreciate audit staff's efforts to provide us with recommendations to further enhance laptop and data security. Our responses to the recommendations appear below:

Recommendation #1

We recommend the agencies:

A. **Routinely monitor laptop security settings to ensure application of security controls.**
B. **Improve and maintain user awareness of laptop security policies and procedures.**

Response:

A. **Concur.** The Department reviewed the laptop audit results provided by the legislative auditors and is developing procedures that address security controls to improve compliance and monitoring of laptop security configurations - including an annual verification by Office of Information Technology (OIT) staff. The Department will implement procedures that provide continual monitoring of security controls in place by March 1, 2012.

B. Concur. The Department is reviewing existing security training programs and will be working to improve training on laptop and data security. OIT staff has prepared and will provide to each laptop user a laptop security guideline outlining laptop security, policies, and procedures. The Department will have enhanced user security training in place by June 30, 2012.

Recommendation #2

We recommend the Department of Labor and Industry, Department of Justice, and Department of Revenue take steps to ensure compliance with state policy by implementing or improving procedures to ensure sensitive data on laptops is encrypted.

Response:

Concur. The Department is evaluating encryption software solutions for laptops and creating policy guidelines for their use to ensure sensitive data on laptops is protected. The Department will complete evaluation of encryption software by June 30, 2012. The Department plans to implement encryption of laptop data by December 31, 2012.

Recommendation #3

We recommend the agencies analyze business need, security risk and cost-effectiveness prior to assignment of laptops.

Response:

Concur. The Department recently implemented a process for managers and OIT staff to evaluate the business needs for the use of laptops. The Department will continue to evaluate our business needs for laptop as part of the annual computer replacement cycle in an effort to reduce the number of laptops allocated to users. This recommendation is currently in implementation.

Sincerely,

Keith Kelly, Commissioner

Cc: George Parisot, Chief Information Officer

DEPARTMENT OF PUBLIC HEALTH AND HUMAN SERVICES

Brian Schweitzer
GOVERNOR

Anna Whiting Sorrell
DIRECTOR

STATE OF MONTANA

www.dphhs.mt.gov

PO BOX 4210
HELENA, MT 59604-4210
(406) 444-5622
FAX (406) 444-1970

January 25, 2012

Tori Hunthausen
Deputy Legislative Auditor
Legislative Audit Division
Room 160, State Capitol Building
PO Box 201705
Helena, Montana 59620-1705

Dear Ms. Hunthausen:

The Department of Public Health and Human Services has reviewed the Improving Controls Over Security of Laptop Data (11DP-12) completed by the Legislative Audit Division. Our response to each DPHHS recommendation is as follows:

Recommendation #1:

We recommend the agencies:

A. Routinely monitor laptop security settings to ensure application of security controls.

DPHHS has implemented monitoring tools to ensure that laptops and computers are compliant. Tools used include ESET virus scan product that provides information on computer/laptop virus level, Configuration Manager software that provides information on HHS computer software level including windows update level, and Guardian Edge encryption software.

DPHHS is also upgrading computers to the Windows 7 operating system. Windows 7 has enhanced security controls allowing for better policy enforcement and security. Approximately 20% of the agency has been converted to Windows 7; the remainder will be converted by July 2013.

B. Improve and maintain user awareness of laptop security policies and procedures

DPHHS has expanded all aspects of information security training, including laptop security. The training plan includes new employee orientation, annual training, management training, email reminders, and specifically tailored training delivered as needed.

Recommendation #3:

We recommend the agencies analyze business need, security risk, and cost effectiveness prior to the assignment of laptops.

DPHHS has updated its procurement process for laptop purchases. New laptop purchases now require a justification for the need of a laptop over the need of a desktop computer.

We appreciate the effort that your staff put into this audit and look forward to using these recommendations to continue improving our controls over the security of sensitive data on department devices.

Sincerely,

Anna Whiting Sorrell
Director

Cc. Laurie Lamson
Ron Baldwin
Marie Matthews

Montana Department of Revenue

Dan Bucks
Director

Brian Schweitzer
Governor

January 27, 2012

Tori Hunthausen, Legislative Auditor
Legislative Audit Division
Room 160, State Capitol
PO Box 201705
Helena, MT 59620-1705

Dear Ms. Hunthausen:

Thank you for the opportunity to respond to recommendations presented in the January 2012 Information Systems Audit Report entitled Improving Controls Over Security of Laptop Data. The audit reviewed laptop security at the Departments of Justice, Labor and Industry, Revenue and Public Health and Human Services. We appreciate the high quality manner in defining the technical terms in Appendix A of the report and will only define terms not referenced in that section. The department's response to the recommendations as they relate to the Department of Revenue (DOR) are as follows:

Recommendation #1

We recommend the agencies:

A. Routinely monitor laptop security settings to ensure application of security controls.

B. Improve and maintain user awareness of laptop security policies and procedures.

Concur and substantially implemented.

A: The department is already following this recommendation, as we are currently monitoring laptop security settings through patch compliance. Based on patches approved by the State Information Technology Services Division, all DOR end users automatically receive those updates.

B: During the department's New Employee Orientation both the Information Security Manager and Technical Security Manager provide training materials educating new employees on the importance of security awareness. We periodically submit educational articles on security in the department's newsletter and through email. Employees are required to sign disclosure statements annually on computers, use of

the internet and confidentiality. Recognizing there is a need for additional reminders to employees about laptop data security, the department will consider using the annual signing of the disclosure statements as an opportunity to provide an additional reminder at that time. Finally, the department will issue Policy 2.3.1 Security Task Force in the next 10 days that defines the responsibilities of the task force including "developing security training for department staff and contractors".

Recommendation #2

We recommend the Department of Labor and Industry, Department of Justice, and Department of Revenue take steps to ensure compliance with state policy by implementing procedures to ensure sensitive data on laptops is encrypted.

Concur; implementation underway, target completion date of March 30, 2012.

The department purchased the Symantec Endpoint Encryption software on December 21, 2011. This is the same software in use at the Department of Public Health and Human Services. This tool will provide full hard drive encryption that will be implemented on all department laptops which will prevent employees from circumventing this security. We plan to work with the department's Education and Training Unit to develop an education and communication plan for the deployment of this software. The changes require end user education on the initial registration process and password resets, password complexity and screen saver timeouts. In order to successfully deploy this software, DOR IT must build and test the infrastructure while working on the education and communication plan. We anticipate having this software fully implemented by March 30, 2012.

Recommendation #3

We recommend the agencies analyze business need, security risk, and cost-effectiveness prior to assignment of laptops.

Concur and implemented.

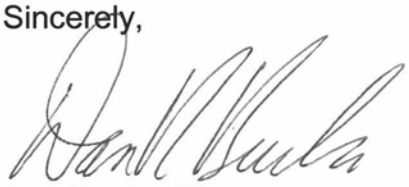
The department already conducts this analysis as part of our laptop assignment process and has been doing so for several years. The analysis weighs the increased costs of a laptop versus the efficiencies gained by the mobility of use and not having to purchase a separate desktop machine. This decision is made by the employee's supervisor and is not at the employee's choosing. In cases where an individual's job duties have changed, they would maintain use of the laptop until they are scheduled for a different computer through the 5 year replacement cycle. Some of the individuals identified in the audit fall into this category.

Although this level of management analysis is in place, DOR recognizes that any process can be improved. Therefore, as part of the education efforts and deploying our new software, we will work with business managers to review the current business

analysis procedures and adjust as necessary. However, we have a high level of confidence that our current process results in proper laptop assignments.

Thank you for allowing us the opportunity to review and respond to the audit report and your recommendations. We appreciate the open discussion we had with you, Angie Grove, Kent Rice, Nathan Tobin and Deon Olson and would like to thank all who participated in the audit for their professionalism and their willingness to work with the department.

Sincerely,



Dan Bucks, Director
PO Box 5805
Helena, MT 59604-5805